Amendments to the Specification:

Please replace paragraph 0002 on page 1, which starts with "The proliferation of ecommerce..." and ends with "...public keys available," with the following amended paragraph:

The proliferation of ecommerce on the Internet has not resulted in a wide diversity of online payment mechanisms. While novel schemes such as Paypal (see "~~http://www.~~paypal.com") have gained in popularity, most business to customer transactions still utilize standard credit card numbers over a Secure Socket Layer (SSL) connection. Multiple use credit cards result in increased risk for the credit card companies, which generally try to insulate their customers from risk by shouldering losses above a nominal sum. Moreover, there are several ways in which SSL can break down in the context of a credit card transaction. While SSL provides for mutual authentication, virtually all consumer oriented web merchants only implement server authentication. Despite the authentication properties of SSL, there is no guarantee that the user is not being fooled by a malicious merchant. Most users do not actually verify the certificates on a secure site; regardless, it is relatively easy for just about anyone to obtain a certificate given the large number of root signing authority public keys available.

Please replace paragraph 0003 on page 1, which starts with "The Secure Electronic Transactions (SET)..." and ends with "...be secure from eavesdroppers," with the following amended paragraph:

The Secure Electronic Transactions (SET) protocol (see "~~http://www.~~setco.org") was designed to protect credit card numbers from malicious parties, and even from malicious merchants. Unfortunately, SET has been seen as requiring too much overhead and the buy-in of too many different parties. Realizing the problem, the credit card companies have started introducing solutions that can be layered over the existing infrastructure. For example, American Express has begun to offer onetime use credit cards, and Visa has

begun to offer limited value gift credit cards. These solutions require users to have a secure interaction with the credit card company, in which a new credit card number is obtained that is linked to an existing account. U.S. Patent No. 5,883,810, to Franklin et al., discloses a variation on this idea wherein users request additional "transaction" numbers from the credit card issuer for each new electronic transaction. The credit card issuer generates a new transaction number for the user and associates the transaction number with a real customer account number in a database record, which is checked when authorization for a particular merchant transaction is sought. Unfortunately, this scheme, as in the case of a user obtaining multiple conventional credit card numbers from an issuer, requires the user to directly contact the credit-card issuer before each transaction in order to obtain a new transaction number. Not only does this require some authenticated interaction with the credit card issuer before the transaction, the interaction must be secure from eavesdroppers.